دانشکده آموزشهای الکترونیکی

پایان نامه کارشناسی ارشد در رشته مهندسی فناوری اطلاعات (تجارت الکترونیک)

بررسی سیستمهای تشخیص نفوذ در پیاده سازی یک الگوریتم هوشمند جهت تجارت الکترونیک

توسط:

احمد رضا موذن جهرمی فرد

استاد راهنما:

دکتر منصور ذوالقدری جهرمی

شهریور ماه 1388

بسم الله الرحمن الرحيم

به نام خدا

بررسی سیستمهای تشخیص نفوذ در پیاده سازی یک الگوریتم هوشمند

جهت تجارت الکترونیک

به وسیله ی:

احمد رضا موذن جهرمی فرد

پایان نامه

ارائه شده به تحصیلات تکمیلی دانشگاه به عنوان بخشی

از فعالیت های تحصیلی لازم برای اخذ درجه کارشناسی ارشد

در رشته ی :

فناوری اطلا عات

از دانشگاه شیراز

شیراز

جمهوری اسلامی ایران

ارزیابی شده توسط کمیته ی پایان نامه با درجه عالی :

دکتر منصور ذوالقدری جهرمی ، دا نشیار بخش مهندسی و علوم کامپیوتر (رئیس کمیته).....

دکتر سراج الدین کاتبی استاد بخش مهندسی و علوم کامپیوتر.....

دکتر محمد هادی صدرالدینی ، دانشیار بخش مهندسی و علوم کامپیوتر.....

شهریور ماه ۱۳۸۸

تقدیم به:

مادر عزیز و مهربانم ...

سپاسگزاری

اکنون که به یاری خداوند متعال موفق به اتمام این پایان نامه شده ام، لازم می دانم از زحمات ارزنده و کمک های بی دریغ استاد گرانقدرم جناب آقای دکتر منصور ذوالقدری جهرمی که در تمامی مراحل پایان نامه از راهنمایی های ارزشمند خود اینجانب را بهره مند ساختند، قدردانی کرده و برای ایشان آرزوی سلامتی و موفقیت کنم.

چکیده

بررسی سیستمهای تشخیص نفوذ در پیاده سازی یک الگوریتم هوشمند جهت تجارت الکترونیک

به وسیله ی :

احمد رضا موذن

هدف سیستمهای تشخیص نفوذ جلو گیـری از دسترسـی غیـر مجـاز کـار بـران بـه سـایتهای کامپیوتری می باشد،با افزایش بنگا ههای تجارت الکترونیکی ، مسئله حفا ظت از این سـا یتهـا به یک مانع اساسی در راه توسعه این سیستمها تبدیل شده است ،مسئله مهم در این رابطه ایـن است که به مرور زمان روشهای جدیـدی بـرای حملـه بـه سـایتهای کـامپیوتری طراحـی مـی شوند،در سالهای اخیر از هوش مصنوعی جهت ارتقاء کارایی سیستمهای تشخیص نفوذ اسـتفاده گردیده است،در این پایان نامه ،از سیستمهای دسته بندی فـازی جهـت معرفـی یـک سیـستم تشخیص نفوذ جدید استفاده شده است ،مزیت عمده سیستم پیـشنهادی ایـن اسـت کـه عمـل تشخیص مهاجم به کمک مجموعه ای از قوانین فازی انجام می شود که بر ای انسان قابل فهـم می باشد. کـــارائی الگـــــوریتم پیشنهادی با انجام یک سری آزمایش بـــر روی مجموعـــه داده KDD99 محاسبه و با چندین روش دیگرکه در تحقیقات گذشته پیشنهاد شده مقایسه گردیـده است.

فهرست مطالب

عنــوان **صفحه**

فهرست شکل ها

عنوان

صفحه

عنوان

صفحه

فهرست جدول ها

عنوان **صفحه**

فصل اول:مقدمه

1-مقدمه

استفاده از روشهای سیستم های تشخیص نفوذ امکان شناسایی کاربرانی که سعی بـه دسترسـی غیر مجاز و یـا تحریـف و یـا تخریـب اطلاعـات در شـبکه هـای کـامپیوتری مبتنـی بـر IP در بنگاههای تجارت الکترونیک را دارند فراهم می کند.

1-1 زمینه طرح مسئله

تهدید بر علیه داده های مشترک رو به افزایش است و بیشتر کمپانی ها بخاطر تهاجماتی که بـه سیستم های کامپیوتری آنها می شود متحمل ضررهای مالی هنگفتی می شوند. و مقدار زیـادی از اطلاعات در معرض سرقت و تخریب قرار می گیر ند.[1]

اطلاعات یکی از مهمترین دارایی هایی یک موسسه مالی یا بنگاه تجاری است. حفاظـت از ایـن دارایی جهت برقرار کردن و ایجاد اعتماد ما بین موسسه مـالی و مـشتریان و سـازگار بـودن بـا قوانین و در نگه داشتن شهرت و اعتبار بنگاه ضروری است. همچنین اطلاعات به موقـع و قابـل اعتماد جهت فرایند تعاملات و پشتیبانی از تصمیمات مشتری توسـط بنگـاه تجـاری ضـروری و اجتناب ناپذیر است. در صورتیکه اطلاعات توسط اشـخاص غیرمجـاز تغییـر داده شـود و یـا در زمان نیاز به آن در دسترس نبا شد. می تواند اعتبار و در آمد بنگاه تجاری و یا موسـسه مـالی را به خطر بیاندازد. ظهور تکنولوژی ارتباطات و اینترنت امکان «اشتراک اطلاعات» و تبادل آسـان اطلاعات را «بین سیستم های کامپیوتری» بوجود آورده اسـت اطلاعـات وفنـاوری هـای نـوین بستری مناسب را برای انجام مبادلات تجاری و ارائه خدمات آنلاین مانند بانکداری الکترونیکی ، تجارت الکترونیکی و دولت الکترونیکی را ایجاد کرده است.

ITیک سکه دو روست: هم فرصت و هم تهدید می باشد اگر به همان نسبتی که به توسعه و همه گیری اش توجه و تکیه می کنیم به امنیت آن توجه نکنیم می تواند به سادگی و در کسری از ثانیه تبدیل به یک تهدید و مصیبت بزرگ شود.

تا اوایل دهه هفتاد فعالیت های مربوط به دسترسی و محافظت از اطلاعات در سازمانها و شرکت ها محدود به محل نگهداری این اطلاعات شامل آرشیو اسناد و شبکه های محلی کامپیوتری بود. در چنین محیط هایی با روشهای حفاظت فیزیکی امنیت سیستم ها و اطلاعات را تا حد بسیار بالایی تامین می کرد. اگر چه مزایای فضای تبادل اطلاعات غیر قابل انکار است ولی اتصالات سیستم های داخلی به شبکه های خارجی و بین المللی و ارائه خدمات و مبادله از طریق این شبکه ها خطرناک است و تهدیدات جدیدی را ایجاد کرده است. مهمترین نگرانی امنیتی مرتبط با سیستم های اطلاعاتی شامل دستیابی نفوذکنندگان به سیستم های اطلاعاتی و سرقت اطلاعات آنها ایجاد و قفه و اختلال در ارائه سرویسهای حیاتی و تغییر یا تخریب اطلاعات است و بدیهی است که در این شرایط روشهای حفاظت فیزیکی به تنهایی قادر به تامین امنیت نخواهد بود و سازمانها ناچار هستند روشهای جدید حفاظت اطلاعات و کنترل دسترسی منابع را در بنگاه تجاری بکاربگیرند.

2-1- تاریخچه سیستم های تشخیص نفوذ

از دهه هشتاد میلادی سیستم های تشخیص نفوذ مورد بررسی قرار گرفت و از آن موقع به بعد تحقیقات و مقالات بسیاری در این خصوص تهیه و ارائه گردیده است. و تعدادی از سیستم های تشخیص نفوذ در هر دو بخش تجاری و آموزش ساخته شده است در گزارش فنی[2] اولین ایده درباره ثبت رویدادها که برای نظارت و کنترل تهدیدها می تواند مورد استفاده قرار بگیرد و تمام روشهای امنیتی مناسب را جهت ردگیری داده های مشکوک که از یک منبع با هویت ناشناس ارسال می شود را ارائه نموده است.

در [3] ایده تشخیص نفوذ بعنوان یک راه حل برای مشکلات حساس امنیتی در سیستم های کامپیوتری عنوان شده است. ایده اساسی این است که مهاجم دارای یک رفتار غیر نرمال در استفاده از کامپیوتر داردسیستم تشخیص نفوذ با استفاده از رفتار یک کاربر عادی طر ح ریزی می شود و هر گونه انحراف از آن به عنوان یک رفتار غیر عادی در نظر گرفته می شود . با روش های آماری[1] رفتار یک کاربر را در صورتیکه از رفتار عادی انحراف دارد به عنوان مهاجم می شناسد. این نوع از سیستم ها احتیاج به ساخت یک مدل از رفتار نرمال کاربر دارد. این روش سعی بر پیش بینی رویدادهای بصری از رویدادهایی کنونی دارد.

در[4] ساختار مبتنی بر مدل[2] را ارائه نمود که سعی در مدل کردن مهاجمین در سطحی بالاتر از ثبت رخدادهای نمونه ای با شکلی مجزا دارد این تکنیک با تکنیک سیستم خبره مبتنی بر قواعد سازی[3] متفاوت است که سعی می کند به شکلی ساده از رویدادهای ثبت شده الگو برداری نماید.

در [5] آنالیز تغییر حالت[4] را عنوان نمود. که رفتارهای مهاجم را که موجب یک سری تغییرات از حالت اولیه امنیتی به حالت مخاطره آمیز می شد به شکلی نموداری نمایش داد. استفاده کردن از وقایع ثبت رویدادها[5] بعنوان ورودی، یک ابزار آنالیز است که در جهت مقایسه تغییر حالت کاربران با نمودار هایی که از تغییرات حالت در حمله های شناخته شده موجود است بکار گرفته می شود.

تکنیکهای علائم هشدار دهنده کلیدی[6] از علائم هشدار دهنده کلیدی کاربر برای تعیین تلاشهای تهاجم گرانه استفاده می کند. در این روش ساختار اصلی تشکیل شده است از

[1] . statically approaches
[2] . model-based approach
[3] . rule-based expert system
[4] . state transition analysis approach
[5] . audit trial
[6] . keystroke monitoring technique

الگوهای که دارای نتایجی بوده اند که منجر به علائم هشدار دهنده شده است و تعدادی از آنها به عنوان علائم هشدار دهنده کلیدی مهاجم شناخته می شود.

در [6] ساختار انطباق الگویی[1] ارائه شده است. در این روش علامت مشخصه مهاجم ها را شناسایی و به صورت رمز در می آید. به صورتی که الگوها دائما خود را با داده های ثبت شده تطبیق دهند. علامت مشخصه ای که الگوبندی شده اند دائما با داده ها مقایسه می شوند و هر داده ای که منطبق با علامت مشخصه بود به عنوان مهاجم شناخته می شوند در سالهای اخیر چندین پایگاه داده از سیستم های تشخیص نفوذ ترکیبی ارائه شده است.

در[7] ایده معماری جدیدی را عنوان کرد که هر دو روشهای سیستم تشخیص نفوذ مبتنی بر رفتارهای غیر نرمال و سوء استفاده[2] را شامل می شد و سیستم تصمیم گیرنده پشتیبان که ترکیب کننده نتایج هر دو روش می باشد را مورد استفاده قرار داد. مدل تشخیص نفوذ مبتنی بر رفتارهای غیر نرمال از ساختار نقشه خودسازماندهی[3] برای مدل سازی رفتار نرمال استفاده می کند. مدل تشخیص نفوذ مبتنی بر سوء استفاده از یک الگوریتم درختی تصمیم[4] برای دسته بندی انواع مختلف مهاجم استفاده می کند. یک سیستم پشتیبان تصمیم مبتنی بر نقش سازی[5] نتایج حاصل از مدلهای مبتنی برسوء استفاده گر را در رفتار غیر نرمال با همدیگر ترکیب می کند.

[1] . pattern matching approach
[2] .misuse
[3] . self organizing map (SOM)
[4] . decision tree algorithm
[5] . Decision support system ((DSS)) agent architecture